METHOD AND APPARATUS FOR MONEY TRANSFERS

This invention relates to method and apparatus for facilitating money transfer. The invention is particularly suitable for inter-country money transfers, but it is not limited exclusively to this.

Money transfer services are offered by a number of organisations, for example banks, the Moneygram organisation, and the Western Union organisation. A transferee wishing to transfer money is able to visit a local authorised agent and arrange for money to be made available for collection by a transferee at another authorised agent or bank, for example, in a different country.

In developing the present invention, it has been appreciated that conventional techniques suffer from certain problems:

(i) Identification of the transferee. Normally, a transferee will be required to present proof of identification, for example, a passport or driving licence, before being permitted to collect the funds. However, there are a large number of countries in which many people do not holds passports or other officially recognisable proof of identification. In such cases, money transfer may be limited to postal transfers. Western Union offers a code-word facility by which a transferor can provide a code word with the initial transfer instructions. The transferee is required to present a matching code word instead of presenting proof of identification.

(ii) Security. Particularly when a code word is used, there is a risk of the transferee, or other parties involved in the money transfer process, committing fraud. It will be appreciated that, especially in certain countries, fraud and corruption may be commonplace, and difficult to control from outside the country. In general, the transferee, and the bank staff in the country of the transferor and the transferee, all have access to the code word and sufficient other information to collect the funds and to complete the transaction (since no proof of identity is required). Such fraud is very difficult to detect and to prevent.

(iii) Accuracy of information. Often, information is passed orally within a transfer organisation by telephone. This can lead to inaccuracies in the information,

particularly when unfamiliar pronunciation is involved, or if two people are not fully conversant in the same language. For example, if a the name of the transferee is misspelt, then it may be impossible for the correct transferee to collect the funds even on presentation of proper identification. Such a common error can only be corrected by the transferor complaining to the transfer organisation, when he is notified of the non-delivery by the transferee; the full transfer details have to be taken again from the transferor to attempt a further transfer.

The present invention has been devised bearing the above problems in mind.

Broadly speaking, a first aspect of the invention is to provide the transferor with a secret identifier code (referred to in preferred embodiments as a party identification code or PIC) which is supplied to the transferor independently of the information exchanged with the transferor when the transferor is making a transfer request (for example, in the preferred embodiment, the PIC is sent to the transferor by post). The identifier code (or at least information related thereto) can be transmitted as part of the money transfer instructions through the money handling authorities. The transferor is required to transmit the secret identifier code to the transferee, and the transferee is, in turn, required to present the identifier code as one of the conditions to be met before the money can be collected by the transferee. Possession of the correct identifier by the transferee represents proof that the transferee has been authorised to receive funds by the transferor.

As used herein the term "money handling authority" refers to any authority empowered to handle money and, where appropriate, refers to any authority empowered to provide funds to a transferee. The term may include, but is not limited to, banks, internet banks, post offices, etc.

Such a technique can avoid the need for the transferee to possess official proof of identification, and can also improve security. In particular, the local handling agents at the point of sale to the transferor will not have access to sufficient information to receive the funds fraudulently.

Preferably, the identifier code (PIC) is allocated for at least one of the parties to the transfer (i.e. the transferor and/or the transferee). In the preferred embodiment, the identifier code (PIC) for the transferor, and the same code is re-used for subsequent transfers from the transferor to any transferee. This avoids the need for new identifier codes to be issued to the transferor for each transaction.

Broadly speaking, a second closely related aspect of the invention is to generate an identifier code (referred in preferred embodiments as a unique transaction code or UTC), and to provide the transferor with the code (to be forwarded by the transferor to the transferee), but provide the money handling authority instructed to handle the transfer with second code (referred in the preferred embodiments as a transaction verification code or TVC) related verifiably to the identifier code. The second code is sufficient to enable the money handling authority to verify that the transferee is authorised to receive the funds upon presentation of the complete code by the transferee. Upon collection of the funds, the money handling authority can return the complete identifier code through the banking system, as evidence that the funds have been collected by the authorised transferee.

Such a technique can provide security against a fraudulent "collection" of the transfer by the money handling authorities instructed to handle the transfer, since the money handling staff will not have access to the complete identifier code to complete validly the transaction by returning the full code as evidence of completion. If the funds are collected fraudulently by a person who has knowledge only of the second code (i.e. the TVC), and has therefore had to add a guessed code to the known code, this will be readily noticeable when the incorrect code is received back from the money handling authority.

Preferably, this aspect of the invention further comprises testing, at least selectively or on demand, the full identifier code information returned for each completed transfer against the originally allocated identifier code to verify that the correct transferee has collected the funds.

Although the above aspects can be used independently, particular advantages can be achieved by using the two aspects in combination. In particular, the technique can then ensure that neither the handling agents at the point of sale, nor the handling agents at the point of collection, possess all of the necessary information properly to complete a transfer. Only the transferor and the transferee possess the necessary codes (i.e. the PIC identifier code of the first aspect, and the UTC identifier code of the second aspect) needed to complete the transfer.

In a closely related aspect, the invention provides a method of generating a first identifier code (UTC in the preferred embodiments) and a second code (TVC in the preferred embodiments) related thereto, the method comprising:

generating the first code such that at least one character thereof represents a function of one or more other characters of the first code;

generating a second code comprising at least one, but not all, of the characters of the first code, and comprising information indicative of the position in said first code of said at least one character and/or of said one or more other characters.

Preferably, the characters of the first code are numeric.

Preferably, the function is a checksum (or sum) function.

Preferably, the second code comprises one or more "blank" characters representing missing character or digit positions of the first code.

Preferably, the function is based on characters in one or more predetermined positions in the first code, and said information represents the position in said first code of the result of the function.

In the preferred embodiment, the function is numeric sum function of the first four digits in the first code, and the information identifies where the result is to be found in the last four digits of the first code; a first character ("F") denotes that the result is in the first one or two digits of the last four; a second character ("M") denotes that the result is in the middle one or two digits of the last four; and a third character ("L") denotes that the result is in the last one or two digits of the last four. It will be

appreciated that other indexing systems could be used, for example, depending on the number of character positions available for the result.

In a closely related aspect, the invention provides a method of testing information provided by a transferee for collection of funds, the method comprising:

receiving transfer instructions including a first party identifier code allocated to at least one of the parties to the transfer, and a second transaction verification code related to a transaction identifier code allocated to the transaction;

(a) comparing the first party identifier code from the transfer instructions with a party identifier code provide by the transferee; and

(b) comparing the second transaction verification code with a transaction identification code provided by the transferee.

Preferably, the method further comprises returning the transaction identification code to the issuing authority as evidence that the transferee is authorised to receive the funds.

Preferably, the transaction verification code contains some, but not all of the characters of the transaction identification code, and the method comprises comparing each known character in the transaction verification code for equivalency with a corresponding character of the transaction identifier code.

Preferably, the transaction verification code includes information associated with the result of a function based on one or more characters of the transaction identification code, and the method comprises testing whether the transaction identification code presented by the transferee matches the function.

In a closely related aspect, the invention provides a money transfer system comprising:

at least one remote input unit operable to generate a money transfer request in accordance with information from a transferor; and

processing means for communicating with each remote unit for receiving and processing money transfer requests received therefrom, the processing means comprising:

means for providing a first identifier code associated with the transaction and/or with the identity of one or more parties to the transfer;

means for outputting first information including the first identifier code, to be communicated directly or indirectly to the transferor independently of the communication with the terminal; and

means for outputting second information to be supplied directly or indirectly to a money handling authority as instructions to effect the transfer for collection, the second information including at least a portion of the first identifier code or information related thereto to enable the authority of the transferee to be verified.

Preferably, the system includes a plurality of terminals. Preferably, the processing means (also referred to herein as the server), is able to communicate with each terminal at various times during a working day, to control the terminals directly, or to upload transfer requests (and any other information) logged by the terminals while off-line (if off-line operation is supported).

In a further closely related aspect, the invention provides a money transfer system comprising:

at least one remote input unit operable to generate a money transfer request in accordance with information from a transferor; and

processing means for communicating with each remote unit for receiving and processing money transfer requests received therefrom, wherein:

the terminal and/or the processing means is operable to output for communication directly or indirectly to the transferor, an identifier code allocated to the money transfer; and

the processing means is operable to output money transfer instructions to be supplied directly or indirectly to a money handling authority as instructions to effect the transfer for collection, the instructions including only a first portion of the identifier code, whereby the money handling authority can verify a portion of the identifier code presented by the transferee.

Preferably, the terminal is operable to output the code to the transferor directly. Preferably, the terminal is operable to communicate the identifier code to or from the processing means.

Preferably, the system comprises means for receiving a full identifier code returned by the money handling authority as evidence of completion of the transfer, and means for comparing the returned identifier code with the originally allocated code for the transaction.

Preferably, the system comprises database means for storing the identifier code allocated to each transaction.

An embodiment of the invention is now described, by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 is a schematic block diagram illustrating the principles used in the embodiment;

Fig. 2 is a schematic diagram illustrating the information used in Fig. 1;

Fig. 3 is a schematic diagram illustrating generation of a UTC and a TVC;

Fig. 4 is a schematic block diagram of a remote input unit;

Fig. 5 is a schematic block diagram of the central server;

Fig. 6 is a flow diagram illustrating operation of the central server;

Fig. 7 is a flow diagram illustrating operation of the second embodiment of terminal;

Fig. 8 is a flow diagram illustrating information exchange between the terminal and the central server during a polling operation; and

Fig. 9 is a flow diagram illustrating operation of the server for handling information from the second embodiment of terminal.

The principles used in this embodiment are first described briefly with reference to Figs. 1 and 2. The system consists of a plurality of remote terminals 10 located, for example, in shops and/or banks within a local community. The terminals 10 communicate with a central processor, also referred to hereinafter as the server 12.

The terminals 10 may, for example, be coupled to the server 12 by conventional telephone modems which call up the server 12 to be controlled by the server 12. In this embodiment, all operations and calculations are performed by the server 12, and the terminal 10 acts as a dumb slave unit, i.e. as a remote input and display device. To improve security, the server 12 may call-back the terminal 10 at a pre-designated telephone number to ensure that third parties cannot break into the server operation.

When a new customer desires to perform a transfer, or desires to be "logged" as a customer for future transfers, this can be done at any terminal 10, which calls the server 12 to perform the process under to server's control. The customer's details including his name and address are inputted through the terminal 10 and recorded by the server 12 in a customer database 12. The local agent gives the customer a swipe card (not shown) which may be coded in any suitable manner, for example, optically, magnetically, or carry an electronic circuit. In this embodiment, the swipe card has a conventional magnetic strip on which is a pre-recorded code uniquely identifying the card. The code also doubles as a unique identification code for the customer (and is referred to later as the CIC, for customer- or card- identification code). To validate the card, the customer or the local agent is required to insert the card into the terminal so that the pre-recorded code can be read by the terminal's card reader (not shown) and communicated to the server 12 to be recorded in the customer database.

Either immediately, or at some time later, the server 12 allocates a party identification code (PIC) for the new customer. The PIC is needed later by a transferee to verify that he has been authorised by the transferor to receive the funds. In this embodiment, the PIC is generated using a random or pseudo random generator, and consists of a numeric code, for example, a four digit code, but an alphanumeric or purely alphabetic code could be used instead. The PIC is printed using a secure postal printer 16, and is posted directly to the customer 14. A significant feature is that the PIC is not communicated through the terminal 10, and so the local agent has no means of accessing a person's PIC to fraudulently intercept transfers.

To perform a transfer, the customer (transferor) 14 presents his swipe card to be inserted into the terminal's card reader. This initiates communication between the terminal 10 and the server 12 so that the transfer details can be inputted to the server 12. The transfer details include the name and address of the transferee, the amount to be transferred, and the name and address of the bank or other money handling authority at which the transferee will collect the transferred funds. The latter information can be selected from a list or menu of allowable collection authorities for any particular country or town.

The server 12 calculates the amount required to be paid by the transferor, which the transferor pays to the local agent. The server 12 then allocates a transaction identification code for the transfer, in the form of a unique transaction code (UTC). In this embodiment, the UTC is based on a pseudo-random code, which is tested to ensure that it uniquely identifies the transfer (at least for the period in which the transfer is valid; the same code is available for re-use after that period). The code is numeric, but in alternative embodiments could be alphanumeric, or purely alphabetic. The server 12 communicates the UTC to the terminal 10, and a hard copy of the transfer details, including the UTC, is printed out by the terminal 10 to be given to the transferor as a receipt.

It is the transferor's responsibility to send the PIC and the UTC to the transferee 18 and to ensure that only the intended transferee receives this information. Normally this would be done by sending the PIC and the UTC by separate routes (depicted as 20a and 20b in Fig. 1), for example, by separate letters, or by communicating one by letter and the other by telephone or telex. The UTC and the PIC together provide the transferee with all of the information needed to validate the transaction, and collect the transferred funds.

To effect the transfer, the server 12 communicates a transfer request 22 directly or indirectly (for example through a remote terminal) to a computer 24 of a domestic bank (assuming that the transfer system is being run by an independent organisation using the bank as an intermediary). The transfer request 22 includes the transfer details

supplied by the transferor, and also includes the PIC and a transaction verification code (TVC). The TVC is related to the UTC to enable verification of the correct UTC when presented by the transferee, but the TVC does not itself contain sufficient information to enable the original UTC to be deduced if it is not known. The bank computer 22 processes the transfer request and communicates the transfer information 26, by conventional bank transfer services, for example by telex, or by SWIFT, to the foreign bank 28 nominated by the original instructions from the transferor 14. The transfer information 26 supplied to the foreign bank includes the PIC and the truncated TVC.

In order to collect the transferred funds, the transferee 18 visits the foreign bank 28 and presents the PIC and full UTC. The PIC provides evidence that the person has been authorised by the transferor to receive funds, and the full UTC provides the necessary authorisation to complete the transaction. The staff at the foreign bank 28 are able to compare transferee's UTC with the TVC with which they have been supplied to verify that the full UTC matches the TVC. The foreign bank 28 then returns the full UTC to the domestic home bank 24 as evidence that the transfer has been properly completed, and that the correct recipient has been paid.

Such a system offers important advantages over conventional techniques:

(a) The transferee does not require any form of personal identification, such as a passport, or a driving licence.

(b) The only parties in possession of all of the necessary information validly to complete a transaction are the transferor, and the transferee. The agents at the point of sale (10) do not have access to the PIC, since this is allocated directly by the server 12, and is communicated to the transferor by post. The staff at the domestic home bank 24 and at the foreign bank 28 have access to the PIC, but do not have access to the full UTC. This will obstruct any fraudulent activity by the handling authorities or agents.

(c) It is the responsibility of the transferor to transmit the PIC and the full UTC to the transferee in a secure manner. If this information is intercepted and the funds are collected fraudulently by a third party, then neither the money handling authorities, nor the money transfer organisation, has to accept liability.

For subsequent transfers from the same transferor 14, the original PIC is reused. The server 12 maintains a database of transferors and the PIC allocated to each. New PIC's are only allocated, printed and posted for new transferors, or if a transferor believes his PIC to have been compromised.

In general, a transferor will only have to notify his PIC to a transferee once. Once the transferee knows the PIC, all he needs to receive funds is the new UTC associated with each individual transaction. This further reduces the chances of information being intercepted between the transferor 14 and the transferee 18.

There are numerous techniques for generating a TVC which relates verifiably to the UTC but does not prejudice the security of the UTC. For example, one technique is to truncate, or blank, one or more digits or characters from the UTC, leaving a code which partly matches the full UTC. The security can be improved by varying the number and/or the positions of the blanked characters, so that a person will not be able to predict which of the characters of the code are already known in the TVC.

Another technique for generating a TVC is generate one or more checksum digits or characters. These can either be included in the UTC, or they can be included only in the TVC. The security can be improved by varying the number and/or the positions of the characters or digits on which the checksum is based, so that a person will not be able to predict which characters represent, or contribute to, the checksum.

In a particularly preferred embodiment, the TVC is generated by a combination of the above two techniques. Referring to Fig 3, the UTC can consist of a 7, 8, 9 or 10 digit code, for example the code illustrated in Fig. 3a. This is based on a pseudo-random number, but tailored such that the sum of the first four digits A is represented somewhere in the last four digits, namely in the first one or two digits B of the last four, or the middle one or two digits C of the last four, or the last digit or digits D. In the illustrated code, the sum (i.e. 8+4+5+9=26) is represented in the middle two digits C of the last four.

Fig. 3b illustrates a first TVC which may be generated from the UTC. The TVC includes some of the original digits, the missing digits being replaced by "blank"

characters. The TVC also includes a prefix code "F", "M" or "L" to indicate whether the sum is to be found in the First, Middle or Last digits of the last four digits. In the present example, the sum is in the middle digits C of the last four, and this is denoted in the TVC by prefix "M". It will be appreciated that the prefix code is only included in the TVC, and not in the UTC.

When the UTC is presented for verification, the local bank can check firstly whether the digits in the UTC agree with the digits already known in the TVC, and secondly, whether the appropriate checksum digits denoted by the TVC's prefix correspond to the sum of the first four digits.

Fig. 3c illustrates a second TVC which may be generated for the same UTC. The prefix code is, of course, the same as that for Fig. 3b, but this example illustrates that a person cannot predict which digits are known in the TVC, since this can vary.

The above scheme represents a balance between security and ease of verification at a remote bank. Other schemes may be used which require computer verification, but this could restrict the banks at which the transferee is able to collect the funds.

Referring to Fig. 4, the remote unit 10 comprises a main processor 30 to which are connected a display screen 32, a keyboard 34, a swipe card reader 38, a receipt printer 40, a customer/transaction logger 41, and a telephone communications modem 44 coupled through an encryption/decryption unit 46 for communicating with the server 12. The display screen may, for example, be a video display unit, or it may be an alphanumeric display, for example, an LCD display. The display is used to present messages and prompts to the customer (transferor) and/or the local agent supervising the remote terminal 10, in response to instructions from the server 12. The details of the transaction and, if the customer is a new customer, the customer's details, are entered using the keyboard 34.

The logger 41 provides a summary of information inputted through the terminal 10 during a working day, so that end-of-day information can be generated and checked by the server 12.

The logger 41 and the encryption/decryption unit 46 are illustrated above as discrete units for ease of description. However, it will be appreciated that these units may be embodied by software running on the main processor 30.

Referring to Fig. 5, the server 12 consists generally of a central processor unit 90 to which are connected a customer database 92, a transaction database 94, a reference database 96, a PIC generator 98, a UTC/TVC generator 100, a secure postal printer 102, an output system 104 (for passing transfer instructions to a bank computer), an input cache 106, and a telephone modem 108 connected through an encryption/decryption unit 110 (which is similar to the encryption/decryption unit 46 described above for the remote terminal 10).

The customer database 92 is a master database of all customers (transferors) who have used the system at any time. For each customer, the database also includes full name and address information, at least limited transaction history, and the customer's PIC and CIC. The transaction database 94 is a master database of the transactions. This includes all pending transactions, and possibly at least a limited history of completed transactions. The information in the transaction database 94 may be archived from time to time to make more memory available for new transactions. The reference database 96 is a master database of the current reference information required for the transactions, including, for example, the countries to which transfers can be sent, available recipient bank details for each country, currency exchange rates and commission rates.

The secure postal printer 102 is of a known type which is able to produce sealed envelopes containing a printed sheet, it being possible to read the sheet only by breaking open the sealed envelope. Such printers are used in applications where it is desired to print information securely to send to a recipient, while ensuring that local staff are unable to read the contents of the envelope.

Fig. 6 illustrates the operation of the server 12 once communication has been established between a terminal 10 and the server 12. Step 122 determines whether the information from the terminal 10 corresponds to a new or existing customer. This is

apparent if the information contains an existing customer identification code CIC. Assuming as a first case that the information does correspond to a new customer, then the process proceeds to step 123 at which the server 12 controls the terminal to prompt for, and return, inputted customer information, including the customer's full name and address. At step 124 a new customer entry is created in the customer database 92.

From step 124, the process proceeds to step 125 at which the server 12 controls the terminal to prompt for a new swipe card to be introduced into the terminal's card reader 38. As explained hereinbefore, the swipe card carries a pre-recorded CIC, which is read by the terminal 10 and returned to the server 12. At step 126, the read CIC is recorded in the customer database. This completes the introduction of a new customer at the terminal 10. The customer can then use the swipe card to initiate a transfer.

At step 127, a PIC is generated for the new customer by the PIC generator 98. As explained previously, the PIC is used later by the recipient to identify himself at his local bank to collect the transferred funds. A separate PIC is generated for each customer. In the present embodiment, the PIC is produced as a random or pseudo-random 4-digit number, so that it is impossible to derive any relationship between the PIC and the customer's details (which might otherwise enable PIC's to be predicted by fraudulent parties). However, in other embodiments, the PIC could be the result of a checksum or hashing function carried out on the customer's name or address, so that it is possible to verify whether given PIC matches given party's name. Alternatively, it is possible to generate a pseudo random PIC using an encryption algorithm which is virtually impossible to reverse or to predict, but which retains a verifiable relationship with the parties names. However, in the present embodiment, it is assumed that it may be difficult to arrange for verification of the PIC by the recipient's bank, and so it is preferred to utilise a completely random PIC.

At step 128, the PIC is recorded in the customer database. The PIC is also printed in a sealed envelope by the secure printer 102, and the envelope is addressed and posted to the customer at his home address identified in the customer information

received from the remote terminal 10 (and now stored in the customer database 92 of the server 12).

It will be appreciated that steps 127 and 128 can be carried out either immediately after communication with the terminal 10, or at some subsequent time when the server 12 may be less busy.

If at step 122 the received information contains an existing CIC (and therefore corresponds to an existing customer, the process proceeds to step 130 at which the customer's PIC is retrieved from the customer database. At step 132, the transfer is analysed to assess whether it is a suspicious transfer which should be stopped for legal reasons. Suspicious transfers may, for example, be detected as any of the following:

(i) transfers greater than a certain allowable amount (which may vary depending on the destination country);

(ii) repeated transfers which accumulate to a sum greater than an allowable amount over a predetermined period (the amount may vary depending on the destination country);

(iii) repeated transfers the frequency of which exceeds an allowable figure (which may very depending on the destination country).

The purpose of step 132 is to provide at least a degree of protection to prevent large scale money laundering or illegal funds transfer from one country to another. If a suspicious transfer is detected, then the transfer process can be aborted, or the server 12 can prompt the terminal 10 that proof of identification is required before the transfer can proceed. Details of the proof of identification (e.g. a passport number) can be entered at the terminal 10 for communication back to the server 12.

At step 134, a check is performed on whether the customer's payment has yet cleared. If cash is used to pay for the transfer, then this step can be omitted. However, if payment has been made by cheque, then no transfer should be authorised until the cheque has been cleared by the customer's bank. If the payment has not yet cleared, then the data is re-stored (for example, in the input cache 106 or in a separate pending store) to be re-processed during the next day's processing.

At step 135, the UTC and the TVC for the transfer are provided. These could either be generated "live", for example, by suitable algorithms, or the UTC and the TVC could be obtained from a supply of pre-generated codes. Such codes could be pre-generated when the server 12 is not busy, for example, overnight, and stored in suitable memory.

At step 136, the UTC is communicated from the server 12 to the terminal 10 to be printed by the terminal's printer 40. This provides the customer (transferor) with the UTC to send to the transferee.

At step 137, the transfer details are issued as a transfer instruction to the intermediary bank. The transfer instructions include the transfer details originally inputted by the customer, the PIC, and the TVC (including the prefix code "F", "M" or "L").

At step 138, the transaction details are stored in the transaction database 94 as a pending transaction, which completes the initial transaction processing. Although not illustrated in the drawings, additional processing can be provided when the foreign bank returns the full UTC as evidence that the transaction has been completed. The returned UTC can be compared to the UTC recorded in the transaction database to verify that the transaction has been completed correctly. Alternatively, this verification step might only be necessary if a transferor complains of non-delivery of funds to the transferee, or of collection by an unauthorised person.

In Fig. 5, the encryption/decryption unit 110, the input cache 106, the PIC generator 98, the UTC generator 100, the TVC generator 101, and the databases 92, 94 and 96 are illustrated as separate "items" from the server processor 90. This is merely to aid description of the invention. It will be appreciated that these functional parts may be implemented by software applications running on the processor.

Although not illustrated in the drawings, it may also be possible for a customer to place a telephone order to a telephone receptionist, who would then enter the transfer details using a dedicated terminal, or directly on to the server 12. The UTC could be issued to the telephone transferor either by telephone, or by means of the secure postal

printer 102. In the latter case, it is preferred that the UTC be printed and posted separately from any communication of a new PIC, to reduce the chances of these items of information being intercepted together.

The above embodiment employs "online" operation of the terminals 10 under the direct control of the server 12. All of the information processing is carried out by the server 12. This can enable relatively inexpensive and straightforward terminals to be used, and it can also enable updated information to be available immediately simply by changing the information and/or the programs on the server.

In an alternative embodiment, it may be desirable to provide at least some of the terminals with a degree of autonomy, for offline operation. Referring to Fig. 4, the terminal 10 is similar to that previously described, but includes the following units (shown in phantom): a UTC/TVC generator 48; a reference database 36; and a customer/transaction database 42. The reference database 36 provides reference information for the remote terminal, such as details of the individual countries to which transfers can be sent, and the individual banks in each country, the exchange and commission rates for each country, and the likely transfer delay for each country (if a calculation of the expected arrival date of the funds is to be provided). The reference database may also include details of public holidays in each country, and the allowable methods of payment by the customer (for example, cash, cheque, credit card, e-cash, mondex, etc.) and the clearance delay for each type of payment (if the calculation of the expected arrival date of the funds is to be provided). The information in the reference database can be updated periodically by the server 12, for example, at the start of a day, or during routine polling of the terminal 10 by the server, as described further below.

The customer/transaction database 46 is used to store details of transfer requests, and details of any new customers, until the information can be uploaded to the server 12 for action.

Referring to Fig. 7, before a new customer can use the transfer system, the customer's details have to be entered into the terminal using the keyboard (step 50).

The customer details include the customer's name and address (or other contact details), so that the secure PIC can be sent later to the customer by the server 12. The customer details are then stored in the customer/transaction database 42 (step 52). Thereafter, the customer is issued with a swipe card (step 54) which carries a unique customer identification code (CIC), as explained previously.

At step 56, the customer (or the local agent) enters details of the desired transfer. Such details include the name and address of the recipient (transferee), the amount to be transferred (in the local currency of the customer), the method of payment by the customer, and the destination country, name and address of the bank or other money handling agent at which the recipient will collect the transferred funds.

At step 58, the processor 30 calculates and displays the value of the funds in the recipient's currency, and the amount of commission charged, based on the information stored in the reference database 36. If desired, the processor may also calculate an estimated date of arrival of the transferred funds at the destination bank, using information in the reference database, and the following formula:

Arrival date = today's date + funds clearance delay + transfer delay + calendar (holiday) delay

If the customer agrees to the transaction and makes payment to the agent, then this is confirmed at step 60. (If the customer declines to proceed, then the process can be aborted at this step.) Thereafter, at step 61 the UTC and TVC for the transfer are provided/generated by the UTC/TVC generator 48. The UTC and TVC can either being generated "live", or a pre-generated UTC and TVC can be retrieved. Such UTC's and TVC's may either be generated by local generators within the terminal, or they may be downloaded from the server 12 as part of the update information for the reference database.

At step 62, the transfer details including the allocated UTC are stored in the customer/transaction database 42 to await uploading to the server 12 for processing.

The transfer details including the UTC are also printed out (step 64) by the terminal's receipt printer 40 to provide a receipt for the customer.

The above method steps apply to a new customer. An existing customer simply inserts his or her swipe card into the terminal's card reader 38 (step 66), at which stage the customer number is read from the card. This provides sufficient information for the server 12 to access the customer's details which are stored in the server 12. After step 66, the process proceeds directly to step 56 for the customer (or agent) to enter the details of the transfer, as described above.

At various intervals during the day, the terminal 10 is polled by the server 12 by telephone, to upload money-transfer information and new customer information to the server 12, and to receive new reference information from the server 12. Referring to Fig. 8, when a telephone call is received from the server 12 (step 70) the process proceeds to step 172 at which the terminal 10 verifies that the call is from the proper server 12, for example, by means of a secret password. The terminal also returns a secret password, so that the server 12 can verify that it is communicating with the proper terminal 10. It will be appreciated that all information sent and received through the telephone line is communicated in encrypted form, so that the information cannot easily be intercepted. At the terminal end, the information is encrypted/decrypted by the encryption/decryption unit 46 connected between the processor 30 and the modem 44.

Following step 72, the terminal waits to receive any new reference information (step 74) for the reference database 36. Such new information may be in the form of a replacement "reference" file to overwrite the entire existing contents of the reference database 36, or it may be in the form of update "packets" to replace only certain information in the reference database. The new information (if any) is then written into the database.

At step 78, the terminal transmits the new contents of the customer/transaction database 42 to the server 12. This new information includes details of any new

customers (including the customer identification number for each new customer), and details of transfer requests entered by the customers.

Step 80 determines whether the terminal has closed at the end of the day and, if so, the process proceeds to step 82 at which end-of-day (EOD) information is transmitted to the server 12. The EOD information includes totals representing the day's transactions and new customers, to provide a cross-check that all of the terminal's information has been validly received by the server 12. This is subsequently cross-checked by the server 12. If the terminal has not yet closed at the end of the day, then the process branches past step 82, to step 84 at which the communication is terminated.

The server 12 will normally poll each terminal 10 at several different times during the day. During each communication session, the terminal transmits only the new information contained in the customer/transaction database 42 (i.e. the information not previously communicated to the server). In this embodiment, the information remains in the customer/transaction database 42 until after the server 12 verifies, for example, by means of the EOD information, that all of the information has been uploaded correctly to the server 12. Such a technique enables all of the information to be uploaded to the server again if necessary, for example, should any discrepancies arise from the EOD information. However, in other embodiments, the customer/transaction database 42 could be cleared after each communication session with the server 12, if desired.

In Fig. 4, the reference database 36, the customer/transaction database 42, the encryption/decryption unit 46 and the UTC/TVC generator 48 have been illustrated as distinct "items" from the processor unit 30. This presentation is merely schematic to aid description of the invention. It will be appreciated that such items may be implemented as application software run by the processor unit. The reference information and the customer/transaction information may be stored as files on conventional mass storage, for example, a semiconductor mass memory or a magnetic disc.

In use, the server 12 polls each remote terminal 10 to download updated reference information to the terminal 10, and to upload new transfer-request information and new-customer information from the terminal. The communication procedure is complementary to that described above with reference to Fig. 8, and so is not expanded further here. The uploaded information is stored temporarily in the input cache 106 until it can be processed by the processing unit 90.

Fig. 10 illustrates the manner in which each "packet" of information from the input cache 106 is processed. Where appropriate the same reference numerals as those in Fig. 6 are used to denote an equivalent operation step. The information is firstly read from the cache 106 at step 120 and, as before, step 122 determines whether the information corresponds to a new customer. Assuming as a first case that the information does correspond to a new customer, then the process proceeds to step 124 at which a new customer entry is created in the customer database 92, containing the CIC read from the input cache.

From step 124, the process proceeds to step 127 at which a PIC is generated for the customer.

At step 128, the PIC is printed in a sealed envelope by the secure printer 102, and the envelope is addressed and posted to the customer at his home address identified in the customer information received from the remote terminal 10 (and now stored in the customer database 92 of the server 12). The PIC is also stored in the customer database 92.

Step 132 represents the first step for processing the transfer after the customer and recipient details have been stored. At step 132, the transfer is analysed to assess whether it is a suspicious transfer which should be stopped for legal reasons, as explained in more detail hereinbefore.

At step 134, a check is performed on whether the customer's payment has yet cleared. Assuming that the payment has cleared, the process proceeds to step 136 at which the transfer details are issued as a transfer instruction to the intermediary bank.

The transfer instructions include the transfer details originally inputted by the customer, the PIC, and the TVC received from he terminal 10.

At step 138, the transaction details are stored in the transaction database 94 as a pending transaction, which completes the initial transaction processing.

If at step 122, the information corresponds to an existing customer, the process proceeds to through step 142 at which the existing PIC for the customer is read from the customer database for re-use. The process then proceeds through step 132 for processing of the transfer details, as described above.

In the above embodiment, the UTC and TVC are allocated to the transaction at the point of sale terminal 10, to provide offline operation of the terminal 10. Although in the illustrated embodiment, the TVC is allocated at the terminal, this could instead be allocated by the server 12, to reduce the risk that the TVC might be available by tapping into the terminal somehow.

In the above embodiments, the PIC is associated only with the transferor. In an alternative form, the PIC could be associated instead with each transferor/transferee pair. Thus instead of a transferor having a single PIC, the transferor would have different PIC's for his different transferees. This could provide additional security if needed, but might require the transferor to remember possibly a large number of PIC's. The customer database would also need to store all of the PIC's for each transferor, and be able to identify subsequent transactions between the same transferor and transferee, in order to use the correct PIC.

In the above embodiments, swipe card is pre-programmed with its CIC, and this is the only information required to be read by the terminal. In other embodiments, the terminal might be equipped with a card reader/writer for writing information to the card as well as reading it from the card. This could enable "favourite recipient" data to be stored on the swipe card in order to simplify the operation for the transferor.

It will be appreciated that the invention, particularly as illustrated in the preferred embodiments, can enable funds to be transferred in a logical and secure, manner, which allows a recipient to receive the funds without having to have official

proof of identity (such as a passport). Only the transferor and the intended transferee have access to sufficient information to complete the transfer, and it is the transferor's responsibility to ensure that the information is sent in a secure manner to the transferee. Neither the local handling agent for the transferor, nor the local handling agent for the transferee, have direct access to sufficient information to complete a valid transfer.

While features believed to be of importance have been identified in the foregoing description, and in the appended claims, the applicant claims protection for any novel idea, feature or combination of features described herein and/or illustrated in the drawings irrespective of whether emphasis has been placed thereon.